



Installation Guide

McAfee® ePolicy Orchestrator® 4.6.0
Software

COPYRIGHT

Copyright © 2011 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface	5
About this guide	5
Audience	5
Conventions	5
What's in this guide	6
Finding product documentation	6
1 Installation requirements and recommendations	7
Hardware requirements and recommendations	7
Software requirements and recommendations	8
Supported server-class operating systems	9
Supported virtual infrastructure software	10
Supported SQL Servers	10
Supported Internet browsers	11
Distributed repository requirements	11
Supported and unsupported products	12
2 Installing McAfee ePolicy Orchestrator software	13
Installation options	13
Things to know before installation	14
About the SQL Server installation documented in this guide	15
About the SQL Server roles required for installation	15
About HTTP port options	16
Performing Express installation	16
Performing Custom installation	18
Performing Cluster installation	20
Installing on Windows Server 2003	21
Installing on Windows Server 2008	25
Testing the ePolicy Orchestrator cluster installation	27
Performing remote Agent Handler installation	28
Installing remote Agent Handlers	28
Completing a first-time installation	29
3 Upgrading McAfee ePolicy Orchestrator software	31
Things to know before upgrading	31
Supported and unsupported products	31
Backing up ePolicy Orchestrator databases and directories	32
Disabling remote Agent Handlers before upgrading	32
Upgrading your ePolicy Orchestrator server	33
Upgrading your ePolicy Orchestrator cluster server	33
Upgrading your remote Agent Handlers	34
4 Uninstalling McAfee ePolicy Orchestrator software	37
Uninstalling Express and Custom installations	37
Uninstalling Cluster installations	38

5	Troubleshooting and log file reference	39
	Common installation messages, and their causes and solutions	39
	Default locations of troubleshooting log files	41
	Index	43

Preface

This guide provides the information you need to install your McAfee product.

Contents

- ▶ *About this guide*
- ▶ *Finding product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses the following typographical conventions and icons.

Book title or Emphasis Title of a book, chapter, or topic; introduction of a new term; emphasis.

Bold Text that is strongly emphasized.

User input or Path Commands and other text that the user types; the path of a folder or program.

Code

A code sample.

User interface

Words in the user interface including options, menus, buttons, and dialog boxes.

Hypertext blue

A live link to a topic or to a website.



Note: Additional information, like an alternate method of accessing an option.



Tip: Suggestions and recommendations.



Important/ Caution: Valuable advice to protect your computer system, software installation, network, business, or data.



Warning: Critical advice to prevent bodily harm when using a hardware product.

What's in this guide

This guide is organized to help you find the information you need. It is organized into chapters that group relevant information together by task, so you can go directly to the topic you need to successfully complete your installation.

In addition to first-time installation instructions for your McAfee ePolicy Orchestrator (McAfee ePO™) software, this guide covers:

- Upgrading your ePolicy Orchestrator software
- Installing in a cluster environment
- Installing and upgrading remote Agent Handlers
- Troubleshooting and log file reference material

Finding product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

- 1 Go to the McAfee Technical Support ServicePortal at <http://mysupport.mcafee.com>.
- 2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	<ol style="list-style-type: none">1 Click Product Documentation.2 Select a Product, then select a Version.3 Select a product document.
KnowledgeBase	<ul style="list-style-type: none">• Click Search the KnowledgeBase for answers to your product questions.• Click Browse the KnowledgeBase for articles listed by product and version.

1

Installation requirements and recommendations

Your environment needs to include specific hardware and software to run McAfee ePolicy Orchestrator 4.6. Review these requirements and recommendations before installing your McAfee ePO software to ensure that your installation is successful.

Contents

- ▶ *Hardware requirements and recommendations*
- ▶ *Software requirements and recommendations*
- ▶ *Supported server-class operating systems*
- ▶ *Supported virtual infrastructure software*
- ▶ *Supported SQL Servers*
- ▶ *Supported Internet browsers*
- ▶ *Distributed repository requirements*
- ▶ *Supported and unsupported products*




Hardware requirements and recommendations

Make sure that your environment conforms to these requirements and recommendations before installing ePolicy Orchestrator software.

Table 1-1 Hardware requirements and recommendations

Component	Requirements and recommendations
Dedicated server	If managing more than 250 systems, McAfee recommends using a dedicated server.
Domain controllers	The server must have a trust relationship with the Domain Controller on the network. For instructions, see the Microsoft product documentation.
File system	NT file system (NTFS) partition recommended.
Free disk space	<ul style="list-style-type: none">• 1.5 GB — First-time installation minimum• 2 GB — Upgrade minimum• 2.5 GB — Recommended minimum
IP address	McAfee recommends using static IP addresses for ePolicy Orchestrator servers. ePolicy Orchestrator supports both IPv4 and IPv6 networks.
Memory	<ul style="list-style-type: none">• 2 GB available RAM minimum• 4 GB available RAM recommended minimum

Table 1-1 Hardware requirements and recommendations (continued)

Component	Requirements and recommendations
Network Interface Card (NIC)	100 Mb or higher  If using a server with more than one IP address, ePolicy Orchestrator software uses the first identified IP address. If you want to use additional IP addresses for agent-server communication, McAfee recommends creating additional Agent Handler groups for each IP address. See <i>Working with Agent Handlers</i> in the <i>ePolicy Orchestrator 4.6 Product Guide</i> or Help for details about setting up Agent Handler groups.
Ports	McAfee recommends avoiding the use of Port 8443 for HTTPS communication. Although this is the default port, it is also the primary port used by many web-based activities, is a popular target for malicious exploitation, and it is likely to be disabled by the system administrator in response to a security violation or outbreak.  Ensure that the ports you choose are not already in use on the server system. Notify network staff of the ports you intend to use for HTTP and HTTPS communication.  Installing the software on a Domain Controller is supported, but not recommended.
Processor	<ul style="list-style-type: none"> • Intel Pentium 4-class or higher • 1.3 GHz or higher

Software requirements and recommendations

Make sure you have the required and recommended software installed on your server system before installing ePolicy Orchestrator software.

Table 1-2 Software requirements and recommendations



Software	Requirements and recommendations
Microsoft .NET Framework 2.0 or later	Required — You must acquire and install this software manually. This software is required if you select an installation option that automatically installs the SQL Server Express 2005 software bundled with this ePolicy Orchestrator software. If this software is missing, you must exit the Setup and acquire and install it manually before proceeding.
Microsoft updates	Recommended — Make sure your Microsoft software is running the latest updates.  Turn off Windows updates before you begin installing or upgrading your software.
Microsoft Visual C++ 2005 SP1 Redistributable	Required — Installed automatically.
Microsoft Visual C++ 2008 Redistributable Package (x86)	Required — Installed automatically.
MSXML 6.0	Required — Installed automatically.

Table 1-2 Software requirements and recommendations (continued)

Software	Requirements and recommendations
Security software	<p>Recommended.</p> <ul style="list-style-type: none"> • Install and/or update the anti-virus software on the server and scan for viruses. • Install and/or update firewall software on the server. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  If McAfee VirusScan® Enterprise 8.5i or 8.7i is running on the system where you are installing the ePolicy Orchestrator software, you must ensure that the VirusScan Enterprise Access Protection rules are disabled during the installation process, or the installation fails. </div>
Supported browser	Recommended — Although it is not a prerequisite for installation, ePolicy Orchestrator software requires the use of a supported browser. You should acquire and install a supported browser manually. For more information, see <i>Supported Internet browsers</i> .
Supported SQL Server	Required — If a supported version of SQL Server has not been previously installed, you can choose to install SQL Server 2005 Express automatically.

Supported server-class operating systems

You can install ePolicy Orchestrator on any supported Microsoft Windows server-class operating systems.

The software is fully supported on the 32-bit and 64-bit (as a 32-bit application) server-class operating systems listed below.

Table 1-3 Supported server-class operating systems

Operating System	32-bit	64-bit	Edition
Windows Server 2003 (with Service Pack 2 or higher)	X	X	<ul style="list-style-type: none"> • Datacenter • Enterprise • Standard
Windows Server 2008 (with Service Pack 2 or higher)	X	X	<ul style="list-style-type: none"> • Datacenter • Enterprise • Standard
Windows Server 2008 R2		X	<ul style="list-style-type: none"> • Datacenter • Enterprise • Standard
Windows 2008 Small Business Server		x	Premium

Operating system language

ePolicy Orchestrator software runs on any supported operating system regardless of the language of the operating system.

The ePolicy Orchestrator user interface has been translated into the languages in the following list. When the software is installed on an operating system using a language that is not on this list, the interface attempts to display text in English.

- Chinese (Simplified)
- Chinese (Traditional)
- English
- French (Standard)
- German (Standard)
- Japanese
- Korean
- Russian
- Spanish

Supported virtual infrastructure software

ePolicy Orchestrator software supports use of several types of virtual infrastructure software.

Supported virtual infrastructure software includes:

- Citrix XenServer 5.5 Update 2
- Microsoft Hyper-V Server 2008 R2
- VMware ESX 3.5 Update 4
- VMware ESX 4.0 Update 1

Supported SQL Servers

ePolicy Orchestrator software requires use of a supported SQL Server. The installation wizard detects whether a supported SQL Server is installed on the server system where you are installing your software. If no SQL Server is present, the wizard prompts you to install Microsoft SQL Server 2005 Express locally.

Table 1-4 Supported SQL Servers

Version	Edition
Microsoft SQL Server 2005 (with Service Pack 3 or higher)	<ul style="list-style-type: none"> • Enterprise Edition • Express Edition • Standard Edition • Work group Edition
Microsoft SQL Server 2008: <ul style="list-style-type: none"> • with Service Pack 1 • with Service Pack 2 • R2 	<ul style="list-style-type: none"> • Enterprise Edition • Express Edition • Standard Edition • Work group Edition

Required SQL Server configuration settings

ePolicy Orchestrator software requires some specific SQL Server configuration settings. For information about working with these settings, see your SQL Server documentation.

Table 1-5 Required SQL Server configuration settings

Configuration	Details
Nested triggers	The SQL Server Nested Triggers option must be enabled.
Database collation	The only database collation supported by ePolicy Orchestrator is the U.S. English default: SQL_Latin1_General_Cp1_CI_AS.
Maintenance settings	McAfee recommends making specific maintenance settings to ePolicy Orchestrator databases. For instructions, see <i>Maintaining ePolicy Orchestrator databases</i> in the Product Guide or Help.

Supported Internet browsers

ePolicy Orchestrator software requires the use of one of these supported Internet browsers.

- Firefox 3.5
- Internet Explorer 7.0
- Firefox 3.6
- Internet Explorer 8.0


Using Internet Explorer enhanced security

If you're using Internet Explorer with enhanced security enabled, you must add the ePolicy Orchestrator server address to your Internet Explorer trusted sites list (formatted as `https://servername`). Failure to do so will display a **You must have javascript enabled to use this product** error message when attempting to log on to the ePolicy Orchestrator server.

Distributed repository requirements

Distributed repositories are used throughout your environment to provide access to important content used by your ePolicy Orchestrator server. Your distributed repositories must conform to these minimum requirements.

Table 1-6 Distributed repository requirements

Component	Requirements
Free disk space	<p>400 MB minimum (800 MB recommended) on the drive where the repository is stored. The required space depends on the amount of data being served.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  The disk space requirement for the distributed repositories on systems where agents are designated as SuperAgents is equal to the disk space available for the master repository. </div>
Memory	256 MB minimum.
Repository hosts	<ul style="list-style-type: none"> • HTTP-compliant servers on Microsoft Windows, or Linux operating systems. • Windows, Linux, or Open Enterprise FTP servers. • Windows, Linux, or UNIX Samba UNC shares. • Systems where a SuperAgent is installed.

Supported and unsupported products

Review the products ePolicy Orchestrator supports before completing your installation or upgrade.

To view an updated list of supported and unsupported products, see one of the following KnowledgeBase articles:

- McAfee ePO Supported Products — [KB69814](https://kc.mcafee.com/corporate/index?page=content&id=KB69814) (https://kc.mcafee.com/corporate/index?page=content&id=KB69814)
- McAfee ePO Unsupported Products — [KB69815](https://kc.mcafee.com/corporate/index?page=content&id=KB69815) (https://kc.mcafee.com/corporate/index?page=content&id=KB69815)

2

Installing McAfee ePolicy Orchestrator software

ePolicy Orchestrator software is installed on a Microsoft Windows server-class operating system using the ePolicy Orchestrator InstallShield Wizard.

The InstallShield Wizard walks you through the configuration steps required to get ePolicy Orchestrator software running. Once you complete the installation process, you can start using the software immediately to get your managed environment set up. Refer to the *ePolicy Orchestrator 4.6 Product Guide* or Help for details about configuring your server and setting up a managed environment.

Contents


- ▶ *Installation options*
- ▶ *Things to know before installation*
- ▶ *Performing Express installation*
- ▶ *Performing Custom installation*
- ▶ *Performing Cluster installation*
- ▶ *Performing remote Agent Handler installation*
- ▶ *Completing a first-time installation*

Installation options

There are three installation options for ePolicy Orchestrator software. Each option walks you through the installation process using the ePolicy Orchestrator InstallShield Wizard.

Use the following table to determine which option is right for your environment.

Table 2-1 Installation options

Installation option	Details
Express	The most direct installation path. Use this option if you want to accept McAfee's default installation settings.
Custom	<p>Customize your installation. Use this option when you want to specify the details of your software installation, including:</p> <ul style="list-style-type: none"> • The destination folder where the software is installed (C:\Program Files\McAfee\ ePolicy Orchestrator\ by default). • The ports used. <div data-bbox="542 569 1524 674" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Installing SQL Server 2005 Express is optional. You can also specify a different supported SQL Server, if installed before you begin the McAfee ePO software installation.</p> </div>
Cluster	<p>Perform a cluster installation. Use this option when you want to install into a cluster environment. Before you begin installing the software:</p> <ul style="list-style-type: none"> • Your Microsoft Cluster Server (MSCS) environment must be set up. • You must have a supported SQL Server installed in a location accessible to your cluster.



If you are upgrading from a prior version of McAfee ePolicy Orchestrator software or are migrating from an evaluation version, see *Upgrading McAfee ePolicy Orchestrator software*.

Things to know before installation

Review this content before beginning your installation.

Be sure that you have read, understood, and complied with the requirements and recommendations detailed in *Installation requirements and recommendations* before you begin the installation.

You should have the following information available during the installation:

- McAfee Product License Key (not required to install an evaluation version of the software).
- Authentication credentials:
 - Windows authentication credentials — You must provide credentials for a domain administrator user account.
 - SQL authentication credentials — Depending on the SQL Server installation options you choose, you might be required to provide SQL authentication credentials. For more information about required SQL Server permissions, see *About the SQL Server roles required for installation*.
- A destination folder for ePolicy Orchestrator software installation (required for Custom and Cluster installations).

- A supported SQL Server (optional for Custom installations, required for Cluster installations).
- If you're using a new SQL Server installed manually, or an existing SQL Server you might need to provide the following details during the installation process (depending on your configuration), on the Database Information page:
 - The name of your SQL Server. Depending on the SQL server's configuration, this name should be formatted using the SQL Server name or the SQL Server name *with* instance name.
 - The dynamic port number, if any, used by your SQL Server.

About the SQL Server installation documented in this guide

ePolicy Orchestrator software requires the use of a supported SQL Server. The only installation scenario described in detail in this guide is a first-time installation of SQL Server 2005 Express.

In this scenario, the InstallShield Wizard installs both the ePolicy Orchestrator software and the SQL Server software on the same system. If you want to install the SQL Server on a different server from the McAfee ePO server, you must install it manually. For more information on installing a different supported SQL Server, see the SQL Server software documentation.



Cluster installation requires you to use a manually installed a SQL Server on a system other than where you install your ePolicy Orchestrator software.

Other relevant SQL Server installations and upgrades

See the Microsoft documentation provided for information about the following installation scenarios:

- Installing SQL Server 2005 or 2008
- Upgrading from MSDE 2000 to SQL Server 2005 or 2008
- Upgrading from MSDE 2000 to SQL Server 2005 Express or 2008 Express



If you are upgrading from MSDE 2000 or SQL 2000, be sure to follow Microsoft's required upgrade scenarios and reboot when requested by the Microsoft updates before installing ePolicy Orchestrator software.

About the SQL Server roles required for installation

If you plan to use an existing SQL Server with your ePolicy Orchestrator software, specific SQL Server roles are required to install successfully.

If you select to use an existing SQL Server, or manually install a new SQL Server, you must provide credentials during the ePolicy Orchestrator installation process for a user account that has been granted the server-role of *dbcreator* on the target SQL Server. This server-role is required for the Setup program to create and add the requisite core ePolicy Orchestrator database object to the target SQL Server during installation.

By default, once the core database is created this user account is granted the database-role of *db_owner* for the core database. After installation is complete, the *dbcreator* server-role can be revoked from this user account. Doing this restricts the account's permissions to only those granted the *db_owner* database-role on the core database.

For more information about the SQL database roles required for your ePolicy Orchestrator server, see *Maintaining your ePolicy Orchestrator databases* in the Product Guide and Help. For a complete discussion of SQL Server roles and permissions, see the product documentation for the supported SQL Server you are using.

About HTTP port options

The ports used by ePolicy Orchestrator software are predefined, and populated by default. Most port designations can be changed only during the installation process.

Review the following table for details about which port assignments you can modify.

Table 2-2 HTTP port options

Port	Default value	Can be changed during installation	Can be changed after installation	Cannot be changed
Agent-to-server communication port	80	X		
Agent-to-server communication secure port	443	X		
Agent wake-up communication port	8081	X	X	
Agent broadcast communication port	8082	X	X	
Console-to-application server communication port	8443	X		
Client-to-server authenticated communication port	8444	X		
Security threats communication port	8801			X
SQL Server TCP port	1200			X

Performing Express installation

The Express installation installs your ePolicy Orchestrator software in the fewest possible steps by automatically accepting the default configuration.

Before you begin

- Be sure that you have read, understood, and complied with the information in *Installation requirements and recommendations*.
- Update the system that will host your ePolicy Orchestrator server with the latest Microsoft security updates, then turn off Windows updates for the duration of the installation process.



We recommend that you monitor the entire installation process. You might be required to restart your system.

Task

- 1 Using an account with local administrator permissions, log on to the Windows server computer to be used as the ePolicy Orchestrator server.
- 2 Run the Setup program.
 - From the product CD: select a language in the ePolicy Orchestrator autorun window, then select **Install ePolicy Orchestrator 4.6**.
 - From software downloaded from the McAfee website: extract files to a temporary location and double-click `Setup.exe`. The executable is located in the file `EPO 4.6.0 <build and package numbers>.zip`.



Do not attempt to run `Setup.exe` without first extracting the contents of the zip file.

The **McAfee ePolicy Orchestrator - InstallShield Wizard** is launched.

- 3 Click **Next** to begin the installation process.
- 4 In the **Setup Type** step, select **Express** and click **Next**.
- 5 In the **Choose Database Option** step, select **Microsoft SQL Express** and click **Next**.
- 6 In the **Install additional software** step, any remaining prerequisites are listed. To install them, click **Next**.




Microsoft .NET Framework 2.0 (or later) is required software when installing SQL Express; it is not installed automatically. If this software is missing, you must exit the Setup and acquire and install it manually before proceeding.

- 7 In the **Database Information** step, specify your Windows authentication credentials and click **Next**.
- 8 If any of the default port assignments are in conflict, you must resolve them by providing alternative ports in the **HTTP Port Information** step.



If no conflicts exist, you will not have the option to modify default port assignments. You must choose the **Custom** installation option if you need to modify port assignments

- 9 In the **Global Administrator Information** step, type the credentials you'll use to log on to your McAfee ePO server when installation is complete, then click **Next**.
- 10 In the **Type License Key** step, type your license key and click **Next**.
If you don't have a license key, you can select **Evaluation** to continue installing the software. The evaluation period is limited to 90 days. You can provide a license key after installation is complete from within the application. For more information, see the Product Guide or Help.
- 11 Accept the **McAfee End User License Agreement** and click **OK**, then click **Install** to begin installing the software.
- 12 When the installation is complete, click **Finish** to exit the InstallShield Wizard.

Your ePolicy Orchestrator software is now installed. Double-click  on your desktop to start using your McAfee ePO server, or browse to the server from a remote web console (`https://servername:port`).

Performing Custom installation

During Custom installation you can modify the installation process at each step. You can specify destination folders and ports using this option.

Before you begin

Be sure that you have read, understood, and complied with the information in *Installation requirements and recommendations*.

If you select to use an existing SQL Server, or manually install a new SQL Server, gather the following information and complete these steps before beginning your installation to ensure that your McAfee ePO software can communicate with the database server:

- 1 Verify that the SQL Browser Service is running.
- 2 Ensure that TCP/IP Protocol is enabled in the SQL Server Configuration Manager.
- 3 Update both the system that will host your ePolicy Orchestrator server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates for the duration of the installation process.



You must monitor the entire installation process when using the **Custom** installation process. You might be required to restart your system.

Task

- 1 Using an account with local administrator permissions, log on to the Windows server computer to be used as the ePolicy Orchestrator server.
- 2 Run the Setup program.
 - From the product CD: select a language in the ePolicy Orchestrator autorun window, then select **Install ePolicy Orchestrator 4.6**.
 - From software downloaded from the McAfee website: extract files to a temporary location and double-click `Setup.exe`. The executable is located in the file `EPO 4.6.0 <build and package numbers>.zip`.



Do not attempt to run `Setup.exe` without first extracting the contents of the zip file.

The **McAfee ePolicy Orchestrator - InstallShield Wizard** is launched.

- 3 Click **Next** to begin the installation process.
- 4 In the **Setup Type** step, select **Custom** and then click **Next**.

5 In the **Choose Database Option** step, select one of the following and click **Next**:

- **Microsoft SQL Express** — Automatically installs SQL Server 2005 Express to the default location defined by Microsoft (C:\Program Files\Microsoft SQL Server).
- **Microsoft SQL Server** — To specify a previously installed SQL database server.

If the server system you are installing on meets any of the following conditions, you cannot install SQL Server 2005 Express locally:



- 16 or more named instances in an existing, locally installed SQL server.
- Any version of a SQL Server locally installed that contains an instance with the name EPOSERVER
- SQL Server 2000 or MSDE 2000 are already installed locally.

6 In the **Install additional software** step, any remaining prerequisites are listed. To install them, click **Next**.



Microsoft .NET Framework 2.0 (or later) is required software when installing SQL Express; it is not installed automatically. If this software is missing, you must exit the Setup and acquire and install it manually before proceeding.

7 In the **Destination Folder** step, click:

- **Change** — Specify a custom destination location for your McAfee ePO software. When the **Change Current Destination Folder** window opens, browse to your desired destination and create any new folders if needed. When finished, click **OK**.
- **Next** — Install your McAfee ePO software in the default location (C:\Program Files\McAfee\Policy Orchestrator\).

8 In the **Database Information** step:

- If you selected **Microsoft SQL Express**, specify your Windows authentication credentials and click **Next**.
- If you selected **Microsoft SQL Server**:
 - a Select the server from the **Database Server** menu.
 - b Specify which type of **Database Server Credentials** to use, then click **Next**:

Windows authentication

- 1 From the **Domain** menu, select the domain of the user account you're going to use to access the SQL Server.
- 2 Type the **User name** and **Password**. If your using a previously installed SQL Server, be sure that the your user account has access.

SQL authentication

- Type the **User name** and **Password** for your SQL Server. Be sure that credentials you provide represent an existing user on the SQL Server with appropriate rights.
The **Domain** menu is greyed out when using SQL authentication




It might be necessary to type the **SQL server TCP port** to use for communication between your McAfee ePO server and database server (default ports for this communication are 1433 or 1434).

- 9 In the **HTTP Port Information** step, review the default port assignments. Click **Next** to verify that the ports are not already in use on this system.



You can modify some of these ports at this time. Once your installation is complete, you can change only the **Agent wake-up communication port** and **Agent broadcast communication port**. If you need to change your other port settings later, you will have to reinstall your McAfee ePO software. For more information about changing port values, see *About HTTP port options*.

- 10 In the **Global Administrator Information** step, type the **Username** and **Password** you want to use for your primary Global Administrator account, then click **Next**.
- 11 In the **Type License Key** step, type your license key and click **Next**.
If you don't have a license key, you can select **Evaluation** to continue installing the software. The evaluation period is limited to 90 days. You can provide a license key after installation is complete from within the application. For more information, see the Product Guide or Help.
- 12 Accept the **McAfee End User License Agreement** and click **OK**, then click **Install** to begin installing the software.
- 13 When the installation is complete, click **Finish** to exit the InstallShield Wizard.

Your ePolicy Orchestrator software is now installed. Double-click  on your desktop to start using your McAfee ePO server, or browse to the server from a remote web console (<https://servername:port>)

Performing Cluster installation

The ePolicy Orchestrator software provides high availability for server clusters with Microsoft Cluster Server (MSCS) software.

Installing the software into your Microsoft Cluster Server environment requires you to take additional steps beyond those needed to complete the Express and Custom installations. The installation process depends on the operating system you are installing on. Cluster installation is supported on Windows Server 2003 or 2008.

Successful installation depends on proper setup of the Microsoft Cluster Server software (MSCS). For more information on MSCS setup, see the Microsoft documentation.

Cluster installation terminology

The following terminology is used in the cluster installation instructions.

Table 2-3 Cluster installation terminology

Term	Definition
Data drive	One of the two drives required by Microsoft Cluster Server and ePolicy Orchestrator software. The data drive is a remote drive that is accessible to all nodes in the cluster, and is the location where you install the ePolicy Orchestrator files.
ePO Virtual IP address resource	The IP address resource that you create as part of the ePolicy Orchestrator cluster installation. This virtual IP address represents the McAfee ePO cluster installation as a whole. References to this IP address point to the currently active node in your cluster.

Table 2-3 Cluster installation terminology (continued)

Term	Definition
ePO Virtual Network Name resource	The Network Name resource that you create as part of the ePolicy Orchestrator cluster installation. This virtual Network Name represents the McAfee ePO cluster installation as a whole. References to this Network Name point to the currently active node in your cluster.
Quorum drive	One of the two drives required by Microsoft Cluster Server software. The quorum drive is where the MSCS files are installed. Don't install any of the ePolicy Orchestrator files on this drive.

Cluster installation requirements and prerequisites

Before you begin your cluster installation, review this list of requirements and prerequisites, and ensure that each is in place or the information is available. These requirements apply to installations on both Windows Server 2003 and 2008.

- Microsoft Cluster Server is set up and running on a cluster of two or more servers.
- A quorum drive is present and configured according to Microsoft guidelines.
- A data drive is present and available to all nodes in the cluster.
- A supported remote SQL Server is configured.
To confirm that the ePolicy Orchestrator software can communicate with this server during installation:
 - Verify that the SQL Browser Service is running.
 - Ensure that TCP/IP Protocol is enabled in the SQL Server Configuration Manager.
- You might need to provide the following details during the installation process (depending on your configuration), on the Database Information page:
 - The name of your SQL Server. Depending on its configuration, this name should be formatted using the SQL Server name or the SQL Server name *with* instance name.
 - The dynamic port number, if any, used by your SQL Server. You must specify the dynamic port number during the installation process, on the Database Information page.

Installing on Windows Server 2003

Installing ePolicy Orchestrator software in a cluster environment running Windows 2003 Server systems requires that you complete each of these tasks in the order listed.

Before you begin

Update the systems that will host your ePolicy Orchestrator server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates for the duration of the installation process.

Tasks

- [Creating the ePolicy Orchestrator application group on page 22](#)
The ePolicy Orchestrator application group is required to separate the ePolicy Orchestrator application from the Microsoft Cluster Services in your cluster environment.
- [Adding the data drive on page 22](#)
The data drive is the location where you install the ePolicy Orchestrator software. Use a remote drive that all nodes in your cluster can access.
- [Adding the ePolicy Orchestrator virtual IP address resource on page 23](#)
The ePolicy Orchestrator virtual IP address resource represents the McAfee ePO cluster installation as a whole. References to this IP address point to the currently active node in your cluster.
- [Adding the ePolicy Orchestrator virtual Network Name resource on page 23](#)
The ePolicy Orchestrator virtual Network Name resource represents the McAfee ePO cluster installation as a whole. References to this Network Name point to the currently active node in your cluster.
- [Installing ePolicy Orchestrator software on each node on page 23](#)
Run the Cluster installation on each of the nodes. To ensure that each node has exclusive access to the quorum and data drives during installation, shut down all other nodes in the cluster.
- [Creating the Generic Service resources on page 24](#)
The Generic Service resources enable the cluster server to control the ePolicy Orchestrator server, by starting and stopping the ePolicy Orchestrator services.

Creating the ePolicy Orchestrator application group

The ePolicy Orchestrator application group is required to separate the ePolicy Orchestrator application from the Microsoft Cluster Services in your cluster environment.

Task

- 1 To open the Cluster Administrator on the active node, click **Start | All Programs | Administrative Tools | Cluster Administrator**.
- 2 Right-click **Groups** in the System Tree, then select **New | Group**.
- 3 In the **New Group** dialog box, type the **Name** and **Description** of the group. For example, ePO. Then click **Next**.
- 4 In the **Preferred Owners** dialog box, identify the owners of the group. Select the desired node under **Available Nodes**, then click **Add**. Repeat until all owners are added, then click **Next**.
- 5 Click **Finish**.

Adding the data drive

The data drive is the location where you install the ePolicy Orchestrator software. Use a remote drive that all nodes in your cluster can access.

Task

- 1 In the Cluster Administrator, right-click the ePO group, then select **New | Resource**.
- 2 In the **New Resource** dialog box, type the **Name** and **Description** of the resource, for example, Data Drive.
- 3 From the **Resource type** drop-down list, select **Physical Disk**.

- 4 Ensure that **ePO** is the selected group, then click **Next**.
- 5 In the **Possible Owners** dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners are added, then click **Next**.
- 6 In the **Dependencies** dialog box, click **Next**.
- 7 In the **Disk** pull-down list, select the disk and click **Finish**.

Adding the ePolicy Orchestrator virtual IP address resource

The ePolicy Orchestrator virtual IP address resource represents the McAfee ePO cluster installation as a whole. References to this IP address point to the currently active node in your cluster.

Task

- 1 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**.
- 2 In the **New Resource** dialog box, type the **Name** and **Description** of the resource, for example, `ePO IP Address`.
- 3 From the **Resource type** drop-down list, select **IP Address**.
- 4 Ensure that **ePO** is the selected group, then click **Next**.
- 5 In the **Possible Owners** dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners are added, then click **Next**.
- 6 No information is required in the **Dependencies** dialog box. Click **Next**.
- 7 Type the virtual IP address and subnet mask for the ePO virtual IP address resource, then click **Finish**.

Adding the ePolicy Orchestrator virtual Network Name resource

The ePolicy Orchestrator virtual Network Name resource represents the McAfee ePO cluster installation as a whole. References to this Network Name point to the currently active node in your cluster.

Task

- 1 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**.
- 2 In the **New Resource** dialog box, type the **Name** and **Description** of the resource, for example, `ePO Server Name`.
- 3 From the **Resource type** drop-down list, select **Network Name**.
- 4 Ensure that **ePO** is the selected group, then click **Next**.
- 5 In the **Possible Owners** dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners have been added, then click **Next**.
- 6 In the **Dependencies** dialog box, select **IP Address**, then click **Next**.
- 7 Provide the virtual server name for the ePolicy Orchestrator virtual Network Name resource, then click **Finish**.

Installing ePolicy Orchestrator software on each node

Run the Cluster installation on each of the nodes. To ensure that each node has exclusive access to the quorum and data drives during installation, shut down all other nodes in the cluster.

Task

- 1 Double click `Setup.exe` in the installation folder.
- 2 Follow the wizard until you reach the **Setup Type** page, then select the **Cluster** option and click **Next**.
- 3 In the **Choose Destination Location** page, specify the path for the shared data drive and click **Next**.



Use this same path for each node.

- 4 In the **Set Virtual Server Settings** page (on the first node only), provide the following identifying information for the McAfee ePO cluster:
 - The ePolicy Orchestrator **Virtual Server IP address**
 - The ePolicy Orchestrator **Virtual Cluster name**
 - The ePolicy Orchestrator **Virtual Cluster FQDN**



This information is automatically provided on subsequent nodes.

- 5 Complete the installation on the first node as described in *Performing Custom installation*.
- 6 Repeat this task for each node in your cluster.

Creating the Generic Service resources

The Generic Service resources enable the cluster server to control the ePolicy Orchestrator server, by starting and stopping the ePolicy Orchestrator services.

You must create and add three Generic Service resources for use with your clustered ePolicy Orchestrator server. Use the following table and task to configure each resource. Be sure to create the resource in the order listed in the table.

Table 2-4 Generic Service resource configurations

Resource	Service	Dependency
ePolicy Orchestrator 4.6.0 Application Server	MCAFEETOMCATSRV250	Data drive
ePolicy Orchestrator 4.6.0 Server	MCAFEEAPACHESRV	ePolicy Orchestrator 4.6.0 Application Server
ePolicy Orchestrator Event Parser 4.6.0	MCAFEEEVENTPARSERSRV	ePolicy Orchestrator 4.6.0 Server

Task

- 1 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**.
- 2 In the **New Resource** dialog box, type the **Name** of the resource.
- 3 Set the **Resource type** to **Generic Service**.
- 4 Set the group to **ePO** and click **Next**.
- 5 In the **Possible Owners** dialog box, ensure that all cluster nodes are added to the **Possible Owners**, then click **Next**.

- 6 In the **Dependencies** dialog box, specify the dependency for each service. Refer to the *Generic Service resource configurations* table above for each dependency.
- 7 In the **Generic Service Parameter** dialog box, type the **Service Name** for each service. Leave the **Start Parameters** field blank, then click **Finish**.

Installing on Windows Server 2008

Installing ePolicy Orchestrator software in a cluster environment running Windows 2008 Server systems requires that you complete each of these tasks in order listed.

Before you begin

Update the systems that will host your ePolicy Orchestrator server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates for the duration of the installation process.

Tasks

- [Creating the ePolicy Orchestrator application group on page 25](#)
The ePolicy Orchestrator application group is required to separate the ePolicy Orchestrator application from the Microsoft Cluster Services in your cluster environment.
- [Creating the Client Access Point on page 25](#)
The Client Access Point defines the ePolicy Orchestrator Virtual IP address and Virtual Network names so your cluster nodes can communicate with your McAfee ePO server.
- [Adding the data drive on page 26](#)
The data drive is the location where you install the ePolicy Orchestrator software. Use a remote drive that all nodes in your cluster can access.
- [Creating the Generic Service resources on page 26](#)
The Generic Service resources enable the cluster server to control the ePolicy Orchestrator server, by starting and stopping the ePolicy Orchestrator services.

Creating the ePolicy Orchestrator application group

The ePolicy Orchestrator application group is required to separate the ePolicy Orchestrator application from the Microsoft Cluster Services in your cluster environment.

Task

- 1 Open the Failover Cluster Management tool on the active node by clicking **Start | Programs | Administrative Tools | Failover Cluster Management**.
- 2 Right-click **Services and Applications** in the cluster management tree, then select **More Actions | Create Empty Service or Application**.
- 3 Right-click **New service or application** and **Rename** the Application Group to **ePO**.

Creating the Client Access Point

The Client Access Point defines the ePolicy Orchestrator Virtual IP address and Virtual Network names so your cluster nodes can communicate with your McAfee ePO server.

Task

- 1 Right-click the **ePO** group and select **Add a resource | Client Access Point**. The **Client Access Point Wizard** appears.
- 2 Type the **ePolicy Orchestrator Virtual Name** in the **Name** field and specify the **ePolicy Orchestrator Virtual IP address** in the **Address** field, then click **Next**. The **Confirmation** page appears.

- 3 Click **Next** to allow the **Client Access Point** to be configured, then click **Finish** when the wizard is complete.
- 4 If the **Client Access Point** is offline, right-click the name and choose **Bring this resource online**.

Adding the data drive

The data drive is the location where you install the ePolicy Orchestrator software. Use a remote drive that all nodes in your cluster can access.

Task

- 1 Right-click the **ePO Application Group** and select **Add Storage**.
- 2 In the **Add Storage** dialog box, select the data drive to be used for your ePolicy Orchestrator installation and click **OK**.

Installing ePolicy Orchestrator software on each node

Run the Cluster installation on each of the nodes. To ensure that each node has exclusive access to the quorum and data drives during installation, shut down all other nodes in the cluster.

Task

- 1 Double click `Setup.exe` in the installation folder.
- 2 Follow the wizard until you reach the **Setup Type** page, then select the **Cluster** option and click **Next**.
- 3 In the **Choose Destination Location** page, specify the path for the shared data drive and click **Next**.



Use this same path for each node.

- 4 In the **Set Virtual Server Settings** page (on the first node only), provide the following identifying information for the McAfee ePO cluster:
 - The ePolicy Orchestrator **Virtual Server IP address**
 - The ePolicy Orchestrator **Virtual Cluster name**
 - The ePolicy Orchestrator **Virtual Cluster FQDN**



This information is automatically provided on subsequent nodes.


- 5 Complete the installation on the first node as described in *Performing Custom installation*.
- 6 Repeat this task for each node in your cluster.

Creating the Generic Service resources

The Generic Service resources enable the cluster server to control the ePolicy Orchestrator server, by starting and stopping the ePolicy Orchestrator services.

You must add three Generic Service resources for use with your clustered ePolicy Orchestrator server. Use the following table and task to configure each resource. Be sure to create the resources in the order they are listed in the table.

Table 2-5 Generic Service resource configurations

Resource	Properties: General tab	Properties: Dependencies tab
ePolicy Orchestrator 4.6.0 Application Server	No changes necessary	Data drive
ePolicy Orchestrator 4.6.0 Server	Remove the Startup parameters and add a blank space. <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;">  Apache will not start with any startup parameters specified, and an empty entry is not permitted. Therefore, a blank space is required. </div>	ePolicy Orchestrator 4.6.0 Application Server
ePolicy Orchestrator Event Parser 4.6.0	No changes necessary	ePolicy Orchestrator 4.6.0 Application Server

Task

- 1 In the Cluster Administrator, right-click the **ePO Application Group** and select **Add a resource | Generic Service**.
- 2 On the **Select Service Wizard**, select a resource and click **Next**.
- 3 In the Confirmation page, click **Next** to allow the service to be created. When the Wizard is complete, click **Finish**.
- 4 Right-click the resource you've just created and select **Properties**. In the **Properties** dialog box set the properties specified in the Generic Service resource configurations table.
- 5 Repeat this task for each generic service resource.

Testing the ePolicy Orchestrator cluster installation

When the ePolicy Orchestrator cluster is set up and online, use this task to ensure that the software functions in a failover situation.

Task

- 1 Restart the system functioning as the active node. The passive node automatically becomes the active node.



The amount of time required for the passive node to become active depends on your unique environment.

- 2 Manually refresh your browser session. If failover is successful, you are redirected to the ePolicy Orchestrator log on page.

Performing remote Agent Handler installation

Each ePolicy Orchestrator server contains a master Agent Handler. Installing additional remote Agent Handlers can help manage an increased number of products and systems managed by a single, logical ePolicy Orchestrator server in situations where the CPU on the database server is not overloaded.

Remote Agent Handlers require the same high-speed network access to your database as the primary ePolicy Orchestrator server.



You can use additional IP addresses for agent-server communication by creating an Agent Handler group, and adding the additional IP address to the virtual IP address input field. For more information, see *Working with Agent Handlers* in the Product Guide or Help.

Installing remote Agent Handlers

You can install Agent Handlers throughout your environment to help manage agent-to-server communication and load balancing. You can install remote Agent Handlers at any time.

Before you begin

Update the system with the latest Microsoft security updates, then turn off Windows updates for the duration of the installation process.


Task

- 1 Open the folder where you extracted the contents of the ePolicy Orchestrator software installation package.
- 2 Copy the `Agent Handler` folder to the intended Agent Handler server system.
- 3 Double-click `Setup.exe` to launch the McAfee Agent Handler InstallShield Wizard. After some installation activities take place in the background, the InstallShield Wizard opens. Click **Next** to begin the installation process.
- 4 After accepting the terms in the license agreement, the **Destination Folder** step opens.
- 5 Accept the default destination or click **Change** to select a different destination, then click **Next**.



The destination path must not contain double-byte characters. This is a limitation of the Apache web server. Using double-byte characters causes the installation to fail and the Apache web server service to fail on startup.

- 6 The **Server Information** step opens.
 - a Type the machine name of the McAfee ePO server with which the Agent Handler must communicate.
 - b Specify which port to use for Agent Handler-to-server communication. The default port is 8444, the same port used for **Client-to-server authenticated communication**.

 Using the default port enables Agent Handler-to-server communication to be performed using only port 8444. You can optionally specify port 8443, the **Console-to-application server communication port**, but doing so requires that port 8444 continues to be available for Agent Handler communication.
 - c Type the **ePO Admin User** name and **ePO Admin Password** of a user with ePolicy Orchestrator Global Administrator privileges.
 - d Click **Next** to use the **ePO Admin** credentials to access the database as well; be sure they are assigned the appropriate SQL Server role and permissions.
 - e Deselect **Use ePO Server's database credentials** and click **Next** to use different credentials to access the database. In the **Database Information** page, specify the following and click **Next**:
 - **Database Server** with instance name. For example, `DB-SERVER\SERVERNAME`.
 - Authentication type.
 - **Domain** name where the database server is hosted.
 - **User name** and **Password**.
 - **Database name** if not provided automatically.
- 7 Click **Install** to start the installation. Once installation is complete, you must enable your remote Agent Handler from within the ePolicy Orchestrator interface. For more information on how to enable your Remote Agent Handler, see *Working with Agent Handlers* in the Product Guide and Help.

Completing a first-time installation

Once you have completed the installation process, you must configure your ePolicy Orchestrator server.

You can use the ePolicy Orchestrator Guided Configuration to set up your server and managed environment. This configuration tool is an overlay to existing features and functionality intended to help you get your server up and running quickly. For more information, see *Using the Guided Configuration tool* in the Product Guide or Help.

3

Upgrading McAfee ePolicy Orchestrator software

You can upgrade version 4.0 Patch 7 or version 4.5 Patch 3 or later of ePolicy Orchestrator software to version 4.6.

Contents

- ▶ *Things to know before upgrading*
- ▶ *Upgrading your ePolicy Orchestrator server*
- ▶ *Upgrading your ePolicy Orchestrator cluster server*
- ▶ *Upgrading your remote Agent Handlers*

Things to know before upgrading

To successfully complete an upgrade, you need to prepare your environment. Review this content before beginning your upgrade.

You need to:

- Review the unsupported products list.
- Back up all ePolicy Orchestrator databases.
- Back up the entire ePolicy Orchestrator directory.
- Disable any remote Agent Handlers in your environment.
- Turn off Windows updates before you begin your upgrade.
- Be sure that you have read, understood, and complied with the requirements and recommendations detailed in *Installation requirements and recommendations* before you begin the upgrade.

Supported and unsupported products

Review the products ePolicy Orchestrator supports before completing your installation or upgrade.

To view an updated list of supported and unsupported products, see one of the following KnowledgeBase articles:

- McAfee ePO Supported Products — [KB69814](https://kc.mcafee.com/corporate/index?page=content&id=KB69814) (https://kc.mcafee.com/corporate/index?page=content&id=KB69814)
- McAfee ePO Unsupported Products — [KB69815](https://kc.mcafee.com/corporate/index?page=content&id=KB69815) (https://kc.mcafee.com/corporate/index?page=content&id=KB69815)

Backing up ePolicy Orchestrator databases and directories

Before you upgrade your software, back up all ePolicy Orchestrator databases, as well as the ePolicy Orchestrator directory.

Details on performing these tasks are available in the following KnowledgeBase articles:

- ePolicy Orchestrator 4.0 — [KB51438](https://kc.mcafee.com/corporate/index?page=content&id=KB51438) (https://kc.mcafee.com/corporate/index?page=content&id=KB51438)
- ePolicy Orchestrator 4.5 — [KB66616](https://kc.mcafee.com/corporate/index?page=content&id=KB66616) (https://kc.mcafee.com/corporate/index?page=content&id=KB66616)

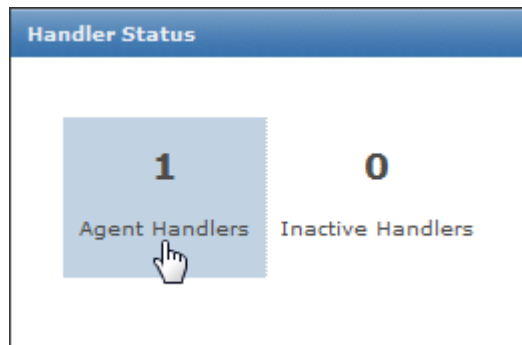
Disabling remote Agent Handlers before upgrading

If you're upgrading from ePolicy Orchestrator 4.5 and you use remote Agent Handlers in your environment, you must disable them in order to successfully complete your upgrade.

Once your remote Agent Handlers are disabled, you can upgrade your server. Once complete, you also need to upgrade your Agent Handlers. See *Upgrading remote Agent Handlers* for more information.

Task

- 1 In the ePolicy Orchestrator 4.5 software interface, click **Menu | Configuration | Agent Handlers**, then click the **Agent Handlers** link in the **Handler Status** monitor to open the **Handler List** page.



- 2 In the **Handler List** page, click **Disable** for each remote Agent Handler you have installed.
- 3 Log on to the system where the Agent Handler is installed, then open the Windows **Services** panel and stop the **McAfee Event Parser** and **McAfee Apache** services.



For more information on using the Windows **Services** panel, see your Microsoft software product documentation.

Upgrading your ePolicy Orchestrator server

You can upgrade your ePolicy Orchestrator server from version 4.0 Patch 7 or version 4.5 Patch 3 or later to version 4.6.

Before you begin

Update the system that hosts your ePolicy Orchestrator server with the latest Microsoft security updates, then turn off Windows updates for the duration of the installation process.



McAfee recommends that you monitor the upgrade process. You might be required to restart your system.

The default location of ePolicy Orchestrator software is:

- 32-bit — C:\Program Files\McAfee\ePolicy Orchestrator
- 64-bit — C:\Program Files (x86)\McAfee\ePolicy Orchestrator

Task

- 1 Log on to the desired system using an account with local administrator permissions.
- 2 Run the Setup program.
 - From the product CD: select a language in the ePolicy Orchestrator autorun window, then select **Install ePolicy Orchestrator 4.6**.
 - From software downloaded from the McAfee website: go to the location containing the extracted files and double-click `Setup.exe`.



If any prerequisite software is missing from the installation target computer, a list of those items appears. Click **Next**. The installation process for each software item listed begins automatically.

- 3 In the Welcome window of the installation wizard, click **Next**. A warning message lists which products are no longer supported with this version of the software. These products are not migrated to the ePolicy Orchestrator 4.6 repository.
- 4 In the **Global Administrator Information** dialog box, type the user name and password of the Global Administrator for the current server, then click **Next**.
- 5 In the **Ready to Install the Program** dialog box, click **Install** to begin the installation.
- 6 In the **InstallShield Wizard Completed** dialog box, click **Finish** to complete the installation.

Upgrading your ePolicy Orchestrator cluster server

Upgrading your ePolicy Orchestrator software in a cluster environment requires special consideration.

Before you begin

If you are upgrading to version 4.6 of the ePolicy Orchestrator software, and your current environment is not supported by this version, you must take the necessary steps to upgrade your environment before upgrading your ePolicy Orchestrator software.

You can upgrade your ePolicy Orchestrator cluster server from version 4.0 Patch 7 or version 4.5 Patch 3 or later to version 4.6 of the software.



Upgrading from ePolicy Orchestrator software 4.0 Patch 7 is supported only on 32-bit server-class operating systems.

Task

1 From the active node, open the **ePO group** in your Windows Cluster Management tool (2003: Cluster Administrator; 2008: Failover Cluster Management). Take each of the following Generic Service resources offline, then delete them:

- McAfee ePolicy Orchestrator 4.x.x Server
- McAfee ePolicy Orchestrator 4.x.x Application Server
- McAfee ePolicy Orchestrator 4.x.x Event Parser

Do not modify the following resources, which are required for a successfully upgrade:



- Data drive
- ePolicy Orchestrator virtual IP address
- ePolicy Orchestrator virtual Network Name

2 Open the Services Control Manager and ensure that the following services are running:

- McAfee ePolicy Orchestrator 4.x.x Server
- McAfee ePolicy Orchestrator 4.x.x Application Server
- McAfee ePolicy Orchestrator 4.x.x Event Parser

Repeat this step on each node before you begin installing your new software.

3 Install your new ePolicy Orchestrator software on each node.



If you're upgrading from version 4.5, consider the node order in which you originally installed version 4.5. You must begin your upgrade on the same node as the original installation. For example, if you installed ePolicy Orchestrator software version 4.5 on nodes A, B, and C, in that order, you must upgrade node A first. The order in which you upgrade subsequent nodes does not matter.

For detailed installation steps, see *Installing ePolicy Orchestrator software on each node* under *Performing Cluster installation*.

4 After completing installation on each node, create the new Generic Service resources for version 4.6 of the software. Configuration for these resources depends on your operating system. For operating system specific configuration details, see *Creating the Generic Service resources* under *Installing on Windows Server 2003* or *Installing on Windows Server 2008*.

Upgrading your remote Agent Handlers

When you upgrade your ePolicy Orchestrator server software, you must also upgrade any remote Agent Handlers installed throughout your environment. Agent Handlers must be upgraded separately.

Remote Agent Handlers installed with previous versions of your software are not compatible with this new version, and are not upgraded automatically.

The upgrade process is a streamlined version of the procedure used for first-time installation of a remote Agent Handler, detailed in *Installing remote Agent Handlers* under *Installing McAfee ePolicy Orchestrator software*.

Task

- 1 Copy the `Agent Handler` folder included in the ePolicy Orchestrator software installation package to the target system.
- 2 Double-click `Setup.exe` to launch the McAfee Agent Handler InstallShield Wizard.
- 3 Click **Next** to begin the upgrade process.
- 4 Accept the license agreement and click **OK**.
- 5 Click **Install** to begin the installation.
- 6 The InstallShield Wizard will complete the installation without any additional input. When the wizard is complete, click **Finish**. Once the upgrade is complete, you must enable your remote Agent Handler from within the ePolicy Orchestrator interface. For more information on enabling your Remote Agent Handler, see *Working with Agent Handlers* in the Product Guide and Help.

4

Uninstalling McAfee ePolicy Orchestrator software

Uninstalling your ePolicy Orchestrator software requires specific steps. Refer to these topics to complete the uninstall process.



If you intend to reinstall ePolicy Orchestrator software later, and want to manage agents deployed by the current installation, you must back up your agent-server communication keys. You cannot restore these keys later.

Contents

- ▶ [Uninstalling Express and Custom installations](#)
- ▶ [Uninstalling Cluster installations](#)

Uninstalling Express and Custom installations

Uninstalling the ePolicy Orchestrator software for Express and Custom installations requires specific consideration of your database.



If you used the Setup program to install SQL 2005 Express, you can remove the database added to that SQL Server when you remove the ePolicy Orchestrator software.

Task

- 1 Close all database management software.
- 2 On the system where your ePolicy Orchestrator server is installed, open the Windows **Control Panel** and uninstall the software:
 - On Windows Server 2003, click **Add or Remove Programs | McAfee ePolicy Orchestrator | Change/Remove**.
 - On Windows Server 2008, click **Programs and Features | McAfee ePolicy Orchestrator | Uninstall/Change**.
- 3 The **Remove McAfee ePolicy Orchestrator** dialog box opens. Select whether to **Also remove the ePolicy Orchestrator database**, then click **Remove**.



You must supply credentials granted sufficient permissions to remove the database. If the provided credentials are not sufficient, you can select to complete the uninstall process without removing the database. For more information about SQL Server permissions, see *Maintaining your ePolicy Orchestrator databases* in the Product Guide and Help.

Uninstalling Cluster installations

Uninstalling ePolicy Orchestrator from a cluster environment requires that you take specific steps, depending on which server-class operating system you are running.

Task

- 1 Open the **Windows Cluster Administrator/Management** tool and set all McAfee ePO services to offline:
 - On Windows Server 2003, click **Start | Program Files | Administrative Tools | Cluster Administrator**.
 - On Windows Server 2008, click **Start | Programs | Administrative Tools | Failover Cluster Management**.
- 2 In the McAfee ePO application group, right-click each of the McAfee ePO resources and select **Delete**.
- 3 Open the **Windows Control Panel** and uninstall the software:
 - On Windows Server 2003, click **Add or Remove Programs | McAfee ePolicy Orchestrator | Change/Remove**.
 - On Windows Server 2008, click **Programs and Features | McAfee ePolicy Orchestrator | Uninstall/Change**.
- 4 Repeat this task on each node in your cluster.

5

Troubleshooting and log file reference

The most common messages that appear while installing McAfee ePolicy Orchestrator during an installation and their solutions are listed here. Use this information to troubleshoot problems with your installation.

If you are unable to resolve an issue using the information in this table, contact McAfee Technical Support after you have taken the steps described below:

- Verify that you have met the minimum installation requirements.
- Review the *ePolicy Orchestrator 4.6 Release Notes* ([Readme.html](#)) for any known installation issues.
- Verify that the account you used to log on to the computer where you are installing the software has full administrator permissions to that computer.
- Collect the exact text of all messages, and be sure to write down any message codes that appear.
- Gather the installation log files.

Contents

- [Common installation messages, and their causes and solutions](#)
- [Default locations of troubleshooting log files](#)

Common installation messages, and their causes and solutions

ePolicy Orchestrator software provides feedback during installation that might require additional action. Review this table for more information on actions required if these messages appear.

Message	Cause	Solution
You are attempting to upgrade from a product version that is not supported. For a complete list of upgrade requirements, see the <i>McAfee ePolicy Orchestrator Software 4.6 Installation Guide</i> .	No version of ePolicy Orchestrator software has been installed on this computer. You can only upgrade from McAfee ePolicy Orchestrator software version 4.0 Patch 7 or version 4.5 Patch 3 or later.	See <i>Installing McAfee ePolicy Orchestrator software</i> in this guide and select an appropriate installation option.
Internet Explorer 7.0 or later, or Firefox 3.5 needs to be installed for this installation to continue.	The computer where you are attempting to install the software is using a non-supported version of the browser.	Install a supported Internet browser before continuing. For more information, see <i>Supported Internet browsers</i> .
Another instance of the ePolicy Orchestrator installer is already running.	The ePolicy Orchestrator 4.6 Setup program is already running. You cannot run more than one instance of Setup at a time.	Allow the first instance of the installer to complete, or stop the first instance and restart your installation.

Message	Cause	Solution
For security reasons, McAfee does not allow blank passwords. Please type a valid password to continue.	The Password box is blank.	Specify the password of the user account that you want to use.
McAfee recommends that you set the video display resolution to 1024x768 or higher.	The computer where you are attempting to install the software does not meet the minimum monitor resolution requirement.	Change the monitor resolution to 1024x768 or higher, then continue the installation. Otherwise, you might not be able to view the entire application window after you start the software. For instructions on changing the monitor resolution, see the Windows Help File (click Start , then select Help).
McAfee recommends that you install the software on a computer with at least 2 GB of RAM.	The computer where you are attempting to install the software does not meet the minimum memory requirement.	Add additional memory to your system or select a different system for installation that has at least 2 GB of RAM.
ePolicy Orchestrator 4.6 software requires that your computer is running Windows Server 2003, or Windows Server 2008.	The computer where you are attempting to install the software is using a non-supported version of the operating system.	See <i>Supported server-class operating systems</i> .
Enter a value in the "Agent Broadcast communication" field.	The Agent Broadcast communication port box is blank.	Specify the port number (default is 8082) that the ePolicy Orchestrator server will use to send agent wake-up calls to SuperAgents.
Enter a value in the "Agent-to-Server communication" field.	The Agent-to-Server communication port box is blank.	Specify the port number that the agent will use to communicate with the server.
Enter a value in the "Agent Wake-Up communication" port.	The Agent Wake-Up communication port box is blank.	Specify the port number (default is 8081) that the ePolicy Orchestrator server will use to send agent wake-up calls.
ePolicy Orchestrator must be installed in a folder. Enter a Destination Folder to continue.	The Destination Folder box is blank or shows the root of a drive.	Click Browse to select a location. The default location is: <code>C:\Program Files\McAfee\ePolicy Orchestrator</code> .
Enter a value in the "User Name" field.	The User name box is blank.	Specify the user name of the account that you want to use.
The License file is missing or corrupt. Contact support for assistance.	Setup is unable to read the license information required to install the software.	Contact McAfee Technical Support.
The operating system or service pack you are using is not currently supported. For a complete list of system requirements, see the <i>McAfee ePolicy Orchestrator 4.6 Software Installation Guide</i> .	The computer where you are attempting to install the software is using a non-supported version of the operating system.	See <i>Supported server-class operating systems</i> .
The passwords you typed do not match. Type a valid password to continue.	The value you typed in Password and Confirm Password do not match.	Specify the password of the account that you want to use.

Message	Cause	Solution
The ePolicy Orchestrator license has expired.	Your license to use the software has expired.	Contact your administrator or designated McAfee representative.
This system is not currently configured with a static IP address, which is recommended for the ePolicy Orchestrator server.	The computer where you are attempting to install the software does not use a static IP address. McAfee recommends using static IP addresses for ePolicy Orchestrator servers to improve performance and reduce bandwidth usage.	Specify a static IP address for use with your ePolicy Orchestrator server.
Unable to make a connection to the database server. Verify that you provided the account credentials and database server name correctly, then try again. If this message continues to appear, see the <i>ePolicy Orchestrator 4.6 Installation Guide</i> for more information.	A connection could not be made to the corresponding ePolicy Orchestrator database server.	<ol style="list-style-type: none"> 1 Verify that the Domain, User Name, and Password you provided are typed correctly. 2 Verify that the database server is running. 3 Verify that the user account you provided is valid for the database server.
Unable to connect using the information you provided. Verify that you entered the correct information and try again.	The user account that you specified could not be accessed.	<ol style="list-style-type: none"> 1 Verify that the Domain, User Name, and Password you provided are typed correctly. 2 Verify that the account you used to log on to this computer has access to this domain.

Default locations of troubleshooting log files

ePolicy Orchestrator provides log files that contain important information when troubleshooting installation issues.

Log file name	Log type	File location	Description
AH460-ahetupdll.log	Temporary	%temp% on the Agent Handler server	Logs Agent Handler back-end events.
AH460-Install-MSI.log			
EPO460-Install-MSI.LOG	Install	%temp%\mfelogs	Main log file for the ePolicy Orchestrator 4.6.0 installer.
[ExtensionFileName].cmd	Temporary	%temp%\MFElogs\epO460-troubleshoot\OutputFiles	File created by ePolicy Orchestrator installer, containing the command (sent to Remote-Client) to check in extensions.
dbmExecute.log	Temporary	%temp%MFElogs	Log of migration errors.
EPO460-Checking-Failure.log	Temporary	%temp%MFElogs	List of extensions that have failed to check in.
core-install.log	Install	[InstallDir]\Installer\core	Log file created when the ePolicy Orchestrator installer calls the Orion ANT installer.
epo-install.log	Install	[InstallDir]\Installer\epO	Log file created when the ePolicy Orchestrator installer calls the Mercury ANT installer.

Log file name	Log type	File location	Description
EpoApSvr.log	Primary	[InstallDir]\DB\Logs	Application Server log file. Present only after initial service startup. Output = RManJNI, DalPolicy, SiteMgr, and SiteMgrWrap.
eventparser.log	Primary	[InstallDir]\DB\Logs	Event Parser log file. Present only after initial service startup. Output = EventParser.
server.log	Primary	[InstallDir]\DB\Logs	ePolicy Orchestrator Server Agent Handler and other C++ code log file. Present only after initial service startup. Output = EPOServer, and Mod_EPO.
errorlog.###-##-##-##_##_##	Apache	[InstallDir]\Apache2\logs	Apache2 log file for the Apache service. Present only after initial service startup.
jakarta_service_#####.log	Tomcat	[InstallDir]\Server\logs	Tomcat log file for the Tomcat service. Present only after initial service startup.
localhost_access_log.###-##-##.txt	Tomcat	[InstallDir]\Server\logs	Tomcat log file for the Tomcat service. Present only after initial service startup.
orion.log	Primary	[InstallDir]\Server\logs	Log file used by the McAfee Foundation Services platform and, by default, all loaded extensions. Present only after initial service startup.
stderr.log	Tomcat	[InstallDir]\Server\logs	Tomcat log file for the Tomcat service. Present only after initial service startup The file contains any Standard Error output captured by the Tomcat service.

Table 5-1 File locations in cluster installations

Log file name	Log type	File location
jakarta_service_#####.log	Tomcat	[InstallDir]\Bin\Server\logs
localhost_access_log.###-##-##.txt	Tomcat	[InstallDir]\Bin\Server\logs
orion.log	Primary	[InstallDir]\Bin\Server\logs
stderr.log	Tomcat	[InstallDir]\Bin\Server\logs

Index

A

- about this guide [5](#)
- Agent Handlers
 - installation [28](#)
 - upgrading [34](#)

C

- cluster installation
 - Windows Server 2003 [21](#)
 - Windows Server 2008 [25](#)
- cluster servers
 - installation [20](#)
 - terminology [20](#)
 - testing [27](#)
 - uninstalling [38](#)
 - upgrading [33](#)
- communication ports, See ports
- conventions and icons used in this guide [5](#)

D

- database collation [10](#)
- database servers
 - support for [10](#)
- distributed repositories
 - requirements [11](#)
- documentation
 - audience for this guide [5](#)
 - product-specific, finding [6](#)
 - typographical conventions and icons [5](#)

F

- Firefox [11](#)

I

- installation
 - Agent Handlers [28](#)
 - cluster [25](#)
 - cluster servers [21](#)
 - completing [29](#)
 - custom [18](#)
 - express [16](#)
 - options [13](#)

- installation (*continued*)
 - preparing for [14](#)
 - preparing for, cluster servers [20](#)
 - required SQL Server roles [15](#)
 - servers [13](#)
- Internet browsers
 - support for [11](#)
- Internet Explorer
 - Enhanced Security [11](#)

M

- McAfee ServicePortal, accessing [6](#)
- Microsoft SQL Servers [10](#)

N

- nested triggers [10](#)

P

- ports
 - changing [16](#)
 - default values [16](#)

R

- requirements
 - distributed repositories [11](#)
 - hardware [7](#)
 - operating systems [9](#)
 - software [8](#)
 - SQL Server roles [15](#)

S

- servers
 - installation [13](#)
 - uninstalling [37](#)
 - upgrading [33](#)
 - virtual infrastructure [10](#)
- ServicePortal, finding product documentation [6](#)
- SQL Servers
 - configuration requirements [10](#)
 - installation [15](#)
 - installation requirements [15](#)
 - roles [15](#)

SQL Servers (*continued*)
support for 10
upgrade scenarios 15
support for
Internet browsers 11
operating systems 9
SQL Servers 10
virtual servers 10
supported products 12, 31

T

Technical Support, finding product information 6

U

uninstalling
cluster servers 38
servers 37
upgrading
Agent Handler 34

upgrading (*continued*)
cluster servers 33
preparing for 31
servers 33

V

virtual servers
support for 10

W

what's in this guide 6
Windows Server 2003
cluster installation 21
support for 9
Windows Server 2008
cluster installation 25
support for 9

